CLAIMS

1. A method of communication between a producer node and a consumer node over a high reliability network, the method comprising the steps of:

(a) preparing a message at the producer node, the message including:

i. message data;

ii. a first error detection code (EDC) based on the message data using a first protocol; and

iii. a second EDC based on the message data using a second protocol different than the first protocol;

(b) transmitting the message to the consumer node;

(c) at the consumer node, receiving the message over the network and calculating;

i. an expected first EDC based on the received message data using the first protocol; and

ii. an expected second EDC corresponding to the received message data using the second protocol; and

(d) comparing the expected first and second EDCs to the received first and second EDCs to determine whether data had been corrupted during the transmission of the message.

2. The method as recited in claim 1, wherein step (a) further comprises preparing actual message data and complementary message data.

3. The method as recited in claim 2, wherein the first protocol includes providing a compressed representation of the actual message data, and the second protocol includes providing a compressed representation of the complementary message data.

4. The method as recited in claim 3, wherein the first protocol further comprises dividing the actual message data by a first polynomial key, and dividing the complementary message data by a second polynomial key different than the first polynomial key.

5. The method as recited in claim 2, wherein the first protocol further comprises dividing the actual message data by a polynomial key, and dividing the

complementary message data by the polynomial key.

6. The method as recited in claim 5, wherein the first and second polynomial keys comprise one of base-16 0x137 and 0x13b.

7. The method as recited in claim 2, wherein the first protocol further comprises dividing the complementary message data by a polynomial key, and the second protocol further comprise dividing the complementary message data by a second polynomial key different than the first polynomial key.

8. The method as recited in claim 1, wherein the first protocol further comprises dividing the message data by a polynomial key, and the second protocol further comprise dividing the message data by a second polynomial key different than the first polynomial key.

9. The method as recited in claim 1, further comprising the step of entering a safety state upon detection of corrupted data.

10. The method as recited in claim 1 wherein the network is selected from the group consisting of: Ethernet, DeviceNet, ControlNet, FireWire or FieldBus.

11. The method as recited in claim 1, wherein the first and second EDCs are generated at the producer node.

12. The method as recited in claim 1, wherein the EDSs comprise cyclic redundancy codes.

13. A method of communication between a producer node and a consumer node over a high reliability network, the method comprising the steps of:

(a) providing actual message data;

(b) generating first and second phantom error detection codes (EDCs) a compressed representations related to the actual message data;

(c) generating an overall EDC as a compressed representation of the first and second phantom EDCs;

(c) transmitting a message from the producer node to the consumer node, the message including the actual message data and the overall EDC, but not the first and second phantom EDCs;

(d) at the consumer node, receiving the message over the network and calculating an expected overall EDC; and

(e) comparing the expected EDC to the received EDC to determine whether data had been corrupted during the transmission of the message.

14. The method as recited in claim 13, wherein step (a) further comprises producing complementary message data that includes a systematic alteration of the actual message data

15. The method as recited in claim 14, wherein the second phantom EDC is produced based on the complementary message data.

16. The method as recited in claim 15, wherein step (c)further comprises transmitting the complementary message data to the consumer node.

17. The method as recited in claim 16, wherein step (d) further comprises receiving the actual and complementary message data.

18. The method as recited in claim 17, wherein step (d) further comprises:

(a) calculating a first expected phantom EDC based on the received actual message data and a second expected phantom EDC based on the received complementary data; and

(b) calculating the expected EDC based on the first and second expected phantom EDCs.

19. The method as recited in claim 14, wherein step (b) further comprises generating the first phantom EDC by applying a polynomial to the actual message data, and generating the second phantom EDC by applying the polynomial to the complementary message data.

20. The method as recited in claim 14, wherein step (b) further comprises generating the first phantom EDC by applying a first polynomial to the actual message data, and generating the second phantom EDC by applying a second polynomial to the complementary message data, wherein the second polynomial is different than the first polynomial.

21. The method as recited in claim 20, wherein the first and second polynomials are selected from the group consisting of base-16 0x137 and 0x13b.

22. The method as recited in claim 13, further comprising generating the first phantom EDC by applying a first polynomial to the actual message data, and wherein the second phantom EDC is produced by applying a second polynomial to the actual message data.

23. The method as recited in claim 14, further comprising generating the first phantom EDC by applying a first polynomial to the complementary message data, and wherein the second phantom EDC is produced by applying a second polynomial to the complementary message data.

24. The method as recited in claim 13, further comprising the step of entering a safety state upon detection of corrupted data.

25. The method as recited in claim 13, wherein the network is selected from the group consisting of selected from the group consisting of: Ethernet, DeviceNet, ControlNet, FireWire or FieldBus.